(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－107350

(43)公開日　平成９年(1997)４月22日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７３Ｃ
Ｇ０６Ｆ	12/00	５３７		Ｇ０６Ｆ	12/00	５３７Ｈ
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ｚ
						６２１Ａ

審査請求　未請求　請求項の数６　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平7－261241

(22)出願日　平成７年(1995)10月９日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　滝本　智之　（外１名）

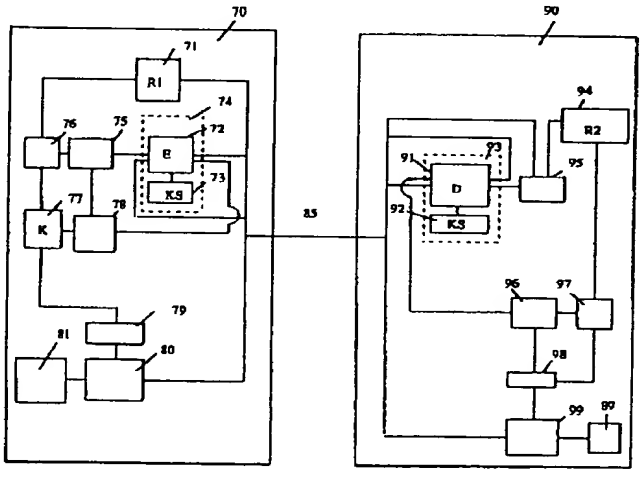
最終頁に続く

(54)【発明の名称】　機器間通信保護装置

(57)【要約】

【課題】　ディジタル著作物再生装置と表示装置との間を結ぶディジタルリンクの認証と暗号化を行ってコピーを防止する。

【解決手段】　暗号アルゴリズムとして「置換」の性質をもつものを考える。このときある暗号化変換E(K,)に対応する復号変換D(K,)は、それ自身暗号変換となる。つまり、D(K,E(K,X))=XのときE(K,D(K,X))=Xとなる。このことにより第１の機器には暗号器Eのみ、第２の機器には復号器Dのみを備えて双方向認証することができる。その結果、(1)１つの機器には暗号器または復号器の一方だけでいいのでコンパクトになり、(2)暗号器は厳重に管理し、復号器は緩い管理にしても、復号器-復号器間の認証通信ができないので全体を厳重に管理できる。



1

【特許請求の範囲】

【請求項１】通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証し通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換であり、一方の機器では前記認証プロトコルにおいて暗号変換のみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なうことを特徴とする機器間通信保護装置。

【請求項２】通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証するとともに共通の暗号鍵を共有しこの暗号鍵を用いて暗号通信を行って通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換であり、一方の機器では前記認証プロトコルにおいて暗号変換のみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なうことを特徴とする機器間通信保護装置。

【請求項３】前記暗号変換および前記認証鍵からなる暗号変換モジュールと前記逆変換と前記認証鍵からなる逆変換モジュールをそれぞれモジュール外部からは前記暗号変換、前記逆変換および前記認証鍵が解析できないような構成とし、一方のモジュールを他方とは異なる管理基準の下に提供することを特徴とする請求項１または請求項２記載の機器間通信保護装置。

【請求項４】前記暗号変換、前記逆変換、および前記認証鍵とはそれぞれ異なる第２の暗号変換とこれに対応する第２の逆変換と第２の認証鍵からなるモジュールをモジュール外部からは前記第２の暗号変換と前記第２の逆変換と前記第２の認証鍵が外部からは解析できないような構成とし、これを通信リンクを介して通信する両方の機器に備え、これを前記認証プロトコルにおいて前記両方の機器において併用するものであり、前記変換モジュールおよび前記逆変換モジュールよりも厳しい管理基準の下に提供することを特徴とする請求項３記載の機器間通信保護装置。

【請求項５】通信リンクにより結合される機器の間で、コマンドフェーズとデータ伝送フェーズを備える機器間通信保護装置であって、前記コマンドフェーズで伝送するコマンドに認証と暗号鍵共有を起動するコマンドと、暗号通信コマンドを追加し、前記コマンドフェーズで認証と暗号鍵の共有を起動するコマンドを指定した場合に、続くデータ伝送フェーズで前記機器の間で前記通信相手の正当性を認証する処理と、その処理の結果として共通の暗号鍵の共有を行ない、次に暗号通信コマンドを指定した場合に、続く前記データ伝送フェーズで、前記

2

共有した暗号鍵を用いてデータを暗号変換して伝送することを特徴とする請求項２記載の機器間通信保護装置。

【請求項６】通信リンクにより結合される機器の間で、一旦リンクを分断して再度リンクを確立する機能を備える機器間通信保護装置であって、分断前に再度リンクを確立する際の通信相手の正当性認証と暗号鍵共有と暗号伝送の、すべてまたは一部に関する情報を共有する手段を有することを特徴とする請求項５記載の機器間通信保護装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はディジタル著作物などを処理する機器が分離しており通信リンクを介して結合されているときその通信路上のデータが不正にコピーされたり改変されたりすることを防ぐ方式と装置に関するものである。

【０００２】

【従来の技術】通信路を介して通信されているデータが通信路上で不正にコピーされたり改変されることを防ぐことが必要となる場合が数多くある。例えば、映画などの著作物がディジタル化されさらに情報圧縮され、さらに光ディスク上にディジタル記録されており、これが光ディスク再生装置により電気情報として取り出され、さらに情報伸長装置により圧縮されていたディジタル情報が伸長され、これが映像音響再生装置により再生される場合を考える。ここで光ディスク再生装置と情報伸長装置は別々の機器として分離しており、その間がディジタル通信路によりデータ通信される場合、この通信データが著作者の許可なくディジタル情報記録装置により記録され、さらにディジタル情報複製装置により複製されるものであれば、その映画の著作物が不正に複製されることになり、著作権の侵害が起こる。従って通信路を介して通信されているデータが通信路上で不正にコピーされることが防がれなければならない。機器内の回路や部品の仕様が一般には公開されないのに対し、データ通信のための電気的特性や信号形式は一般に公開される場合が多いので通信路におけるデータの不正コピーやそれに引き続くデータの改変が大きな問題になる。

【０００３】このような機器間通信保護装置の構成法については従来より様々なものが知られている。最も代表的なものは相手認証技術を用いるものである。これは基本的にはデータを送出する側が受信する側の正当性を認証し、正当な受信者であることが確認できたときのみにデータを送信することによりデータが不正な機器に受信されることがないようにするものである。この場合の受信者のように自らの正当性を証明する側を証明者と呼び、またこの場合の送信者のように相手の正当性を確認する側を認証者と呼ぶ。

【０００４】前述の光ディスク記録再生に関わる機器のような場合、特定の機器の間で認証が行われるというよ

りも、光ディスク関連機器の業界によって定まる規格に従って作成されたかどうかが問題となる。従ってこの場合、「正当性」とは「所定の規格に準拠すること」を意味する。

【０００５】従来の技術の一例として国際標準規格ＩＳＯ／ＩＥＣ９７９８－２に記載される暗号技術を用いた一方向認証方法がある。この認証方法は証明者が認証鍵と呼ばれる秘密のデータを持つことを、その鍵自身を知らせることなく証明者に対して証明することを基本としている。そのためにまず認証者があるデータを選びこれを証明者に対して投げかける。これをチャレンジを呼ぶ。これに対し証明者がある暗号変換を保有し前記認証鍵を用いて前記チャレンジデータを暗号化する。このように暗号化されたデータをレスポンスとして認証者に対して返す。このレスポンスを受信した認証者は前記暗号変換の逆変換である復号変換と認証鍵を共有しており、このレスポンスを前記認証鍵を用いて前記復号変換によって復号する。この結果が前記チャレンジと一致すれば受信者は正規の認証鍵を持つものと判断し、証明者の正当性を認証する。一方向認証とは一方の側がその正当性を他方に証明することを意味している。

【０００６】暗号変換Tとは、鍵情報Kにより定まる平文集合から暗号文集合への写像である。平文をXとしたとき暗号文を T(K,X)と書く。同じ鍵情報Ｋにより定まる暗号文集合から平文集合への写像である逆変換TINVとの間には、

TINV(K,T(K,X)) = X

の関係がある。これは平文Ｘを暗号変換し、これを逆変換すると元に戻ることを意味している。暗号の場合、暗号変換の逆変換を特に復号変換と呼ぶ。暗号変換であるためには鍵Ｋの知識がないときにT(K,X)からXを求めることが必要である。以降では慣例により暗号変換をE(K,)、復号変換をD(K,)と記す。

【０００７】図６は前記規格に記載されている認証方法を実現する装置の一例である。図６において、１０は第１の機器、１１は乱数発生部、１２はある暗号アルゴリズムの復号器、１３は第２の機器の認証鍵K2を格納する第１の認証鍵格納部、１４はデータ比較部、１５は著作物送信ゲート、１６は著作物データ格納部である。１１から１６は第１の機器１０の構成要素である。２０は通信路である。３０は第２の機器、３２は前記暗号アルゴリズムの暗号器、３３は第２の機器の認証鍵K2を格納する第２の認証鍵格納部、３４は著作物データ処理部である。３２から３４は第２の機器３０の構成要素である。

【０００８】この従来の一方向認証方法の動作を図７の動作説明図に従い説明する。

（１）第１の機器１０が通信路２０を介して第２の機器３０に対して著作物データ格納部１６に格納されている著作物データを送信しようとする場合、まず第１の機器１０は乱数発生部１１において乱数Rを生成する。そしてこれをチャレンジデータCHAとして通信路２０に対して送出する。

【０００９】CHA = R

（２）第２の機器３０はこの乱数を受けとると、この乱数を平文とし、第２の認証鍵格納部３３に格納されている認証鍵K2を暗号鍵として暗号器３２により暗号化する。そしてその結果RESをレスポンスとして通信路に対して送出する。

【００１０】RES = E(K2, CHA)

（３）この電文RESを受けとった第１の機器１０はこのレスポンスデータRESを暗号文とし、第２の機器の認証鍵格納部１３に格納されている認証鍵K2を復号鍵として復号部１２において復号する。

【００１１】D(K2,RES) = RR

そしてこの結果をデータ比較部１４において乱数発生部１１に一時保管されている乱数Rと比較する。これが一致すれば通信相手は第２の機器３０の認証鍵を保有するものと考え、通信相手が正当なものであると認証して（４）に進む。一方一致しなければ通信相手が正当なものではないものと判断して処理を中断する。

（４）このように第１の機器１０が第２の機器３０を正当なものとみなせば、第１の機器は著作物データ格納部１６に格納されている著作物データを通信路２０を介して第２の機器３０に伝達する。これを受信した第２の機器３０はこの著作物データを著作物データ処理部３４において処理される。

【００１２】もしも、第２の機器の代わりに第２の機器の認証鍵を有さない第３の機器が通信路２０に接続されている場合、その第３の機器は上記ステップ（２）で正しい値のデータを作成することができない。従って第１の機器は上記ステップ（３）で通信相手が正しくない機器であるものと判断する。このようにして著作権のあるデータは不正な機器に伝送されることがない。

【００１３】なお、第１の機器と第２の機器の間でいつも同じチャレンジとレスポンスデータが用いられるならばこれを利用して不正な第３の機器が第２の機器になりすますことが考えられる。これを避けるために第１の機器からは毎回異なるチャレンジを送る。

【００１４】しかしながら、上記に示したように第１の機器が正規の認証鍵を持つ第２の機器を認証した後著作権データを通信路２０を介して第２の機器に伝送している最中に、この通信路上のデータを抜きとり、これを例えばハードディスク装置に記憶することが考えられる。もちろんこのためには通信路上の信号の電気的特性やデータ形式などの知識が必要であるがこれは特に秘密にされている情報ではないのでディジタルデータの抜きとりは技術的に十分に可能である。同様にしてこのようにハードディスク装置に記憶されているデータを正規の認証鍵を有する第２の機器に対して送出することも可能である。従って、上記の一方向認証方法だけでは著作権デー

5

タの保護は不完全である。この課題を解決するためには、第１の機器が第２の機器の正当性を確認すると同時に第２の機器が第１の機器の正当性を確認することが必要となる。

【００１５】このように上記の一方向認証を組み合わせて双方向認証を行なう方法も上記国際標準規格に述べられている。

【００１６】図８はこの双方向認証方式を実現する装置の一例を示すものである。但し、ここでは双方向認証方式を実現するのみならず、双方向認証の処理の結果、２つの機器にランダムな鍵が共有されるようになっている。この共有鍵はこの認証プロトコルに引続き行なわれる暗号通信のための暗号／復号鍵に用いられるものである。

【００１７】図８において、４０は第１の機器、４１は第１の乱数発生部、４２は第１の暗号アルゴリズムの復号器、４３は第２の機器の認証鍵K2を格納する第１の認証鍵格納部、４４は第１のデータ分離部、４５は第１のデータ比較部、４６は第３の乱数発生部、４７は第２の暗号アルゴリズムの暗号器、４８は第１の機器の認証鍵K1を格納する第２の認証鍵格納部である。４９は第１の共有鍵一時格納部、５０はデータ暗号器、５１は著作物データ格納部、５２は第１のデータ連結部である。４１から５２は第１の機器４０の構成要素である。５５は通信路である。６０は第２の機器、６１は前記第１のアルゴリズム復号器４２に対応する第１の暗号アルゴリズムの暗号器、６２は第２の機器の認証鍵K2を格納する第３の認証鍵格納部、６３は第２の乱数発生部、６４は前記第２の暗号アルゴリズムの復号器、６５は第１の機器の認証鍵K1を格納する第４の認証鍵格納部、６６は第２のデータ分離部、６７は第２のデータ比較部、６８は第２の共有鍵一時格納部、６９はデータ復号器、５８は第２のデータ連結部、５９は著作物データ処理部である。６１から６９、５８、５９は第２の機器６０の構成要素である。

【００１８】この従来の双方向認証方法の動作を図９の動作説明図に従い説明する。

（１）まず、第１の機器４０は第１の乱数発生部４１において乱数R1を生成する。これは第１のチャレンジCHA1としての意味を持つ。そしてこれを通信路５５に対して送出する。

（２）第２の機器６０はこの乱数R1を受けとると、第２の乱数発生器６３において第２の乱数R2を発生し、第２のデータ連結部５８において第１の乱数R1と第２の乱数R2の連結R1||R2を作成する。そしてこれを平文とし、第３の認証鍵格納部６２に格納されている第２の機器の認証鍵K2を暗号鍵として第１の暗号アルゴリズムの暗号器６１により暗号化する。

【００１９】RESCHA = E(K2, R1||R2)

ここでR2は第２のチャレンジとしての意味を持つ。暗号

6

化した結果は第１のチャレンジに対するレスポンスおよび第２のチャレンジの両方の意味を持つ。そしてその結果RESCHAを通信路５５に対して送出する。

（３）この電文RESCHAを受けとった第１の機器４０はこれを暗号文とし、第１の認証鍵格納部４３に格納されている第２の機器の認証鍵K2を復号鍵として第１の復号部４２において復号する。

【００２０】D(K2, RESCHA) = X1

そしてその結果X1を第１のデータ分離部４４に入力する。第１のデータ分離部４４は入力されたデータを第１の乱数部分RR1と第２の乱数部分のデータRR2に分離する。

【００２１】X1 : RR1 || RR2

そして第１の乱数部分のデータRR1を第１のデータ比較部４５に対して送出する。第１のデータ比較部４５はこのデータRR1を第１の乱数発生部４１に一時記憶されている乱数R1と比較する。これが一致すれば通信相手が第２の機器６０の認証鍵K2を持っていることを証明したものと考え、通信相手が間違いなく第２の機器６０であるものと認証し（４）に進む。もしも一致しなければここで認証処理を中断する。

（４）第３の乱数発生部４６は第３の乱数Kを発生する。そして第１のデータ連結部５２は第１のデータ分離部４４において分離された第２の乱数部分のデータRR2とこの乱数Kを連結しその結果RR2||Kを第２の暗号アルゴリズムの暗号器４７に渡す。暗号器４７はこれを平文とし、第２の認証鍵格納部４８に格納されている第１の機器の認証鍵K1を暗号鍵として暗号化する。

【００２２】RES2 = E(K1, RR2||K)

その結果RES2を通信路５５に対して送出する。

（５）この電文を受けとった第２の機器６０はこのレスポンスデータRES2を暗号文とし、第４の認証鍵格納部６５に格納されている第１の機器の認証鍵K1を復号鍵として第２の暗号アルゴリズムの復号部６４において復号する。

【００２３】D(K1, RES2) = X2

そしてその結果X2を第２のデータ分離部６６に入力する。第２のデータ分離部６６は入力されたデータを第２の乱数部分RRR2と第３の乱数部分KKのデータに分離する。

【００２４】X2 : RRR2 || KK

そして第２の乱数部分のデータRRR2を第２の比較部６７に対して送出する。第２の比較部６７はこのデータRRR2を第２の乱数発生部６３に一時記憶されている乱数R2と比較する。これが一致すれば通信相手は第１の機器４０の認証鍵K1を持っていることを証明したものと考え、通信相手が間違いなく第１の機器４０であることを認証する。そして（６）に進む。もしも一致しなければ認証は失敗したものとして認証処理を終る。

（６）第２のデータ分離部で分離された第３の乱数KK

（これはKに等しいことが確認されている）を第２の共有鍵一時格納部６８に設定する。そして第１の機器４０に対して認証した旨の信号を送る。

（７）第２の機器６０から認証した旨の信号を受けた第１の機器４０は第３の乱数発生部４６で生成した乱数Kを第１の共有鍵一時格納部４９に転送する。そしてデータ暗号器５０は著作物データ格納部５１から入力される著作物データをこの乱数Kを暗号鍵として用いて暗号化しその結果を通信路５５に対して送出する。

（８）この電文を受け取った第２の機器６０はデータ復号器６９に入力されるデータを第２の共有鍵一時格納部６８に格納されているデータを復号鍵として復号しこれを著作物データ処理部５９に対して出力する。

【００２５】第１の機器４０と第２の機器６０がどちらも正当なものであれば共有鍵一時格納部６８に格納されているデータは前記第１の共通鍵一時格納部に格納されているデータと等しくなるので（７）のステップで暗号化されたデータが正しく復号される。

【００２６】もしも第１の機器が正規の認証鍵を有し、第２の機器が正規の認証鍵を有していない場合、ステップ（３）で第１の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。また第１の機器が正規の認証鍵を有しておらず、第２の機器は正規の認証鍵を有している場合、ステップ（５）において第２の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断する。このようにして著作権データが不正な機器に流出することとともに不正な機器から正規の機器に流入することが防止できる。

【００２７】また、第１の機器も第２の機器も正当な認証鍵を有している場合で、認証処理が完了し、ステップ（７）（８）において著作権データが通信路上を伝送されているものを電気的にコピーしてディジタル蓄積装置に蓄積したとしてもそのディジタルデータは暗号化されており、無意味なものなので著作権データを有効に保護できる。

【００２８】以上の説明においては第１の機器による第２の機器の認証には第１の暗号アルゴリズムを用い、第２の機器による第１の機器の認証には第２の暗号アルゴリズムを用いるものとした。このように別の暗号アルゴリズムを用いるのではなくそれぞれに同じ暗号アルゴリズムを用いてもよい。この場合、第１の暗号アルゴリズムの復号器４２と第２の暗号アルゴリズムの復号器６４とは同一のものとなる。以下ではこれを復号器と呼ぶ。同様に第１の暗号アルゴリズムの暗号器６１と第２の暗号アルゴリズムの暗号器４７は同一のものとなる。以下ではこれを暗号器と呼ぶ。

【００２９】以上のように暗号アルゴリズムを用いた双方向認証が首尾よく行われるには、第１の機器および第２の機器の内部に格納されている認証鍵が不正を行おうとするものに容易に分からないことが前提となる。このために最も効果的な方法は、上記の暗号器と第１のまたは第２の機器の認証鍵の一対を同じ集積回路の中に封じ込めて実現するものである。こうすれば、その集積回路の解析には多大な労力がかかるので認証鍵が容易には分からないこととなる。同様に復号器と第１または第２の機器の認証鍵の一対を同じ集積回路の中に封じ込める。

【００３０】上記の例では第１の機器では復号器と第２の機器の認証鍵の対、暗号器と第１の機器の認証鍵の対が必要となり、第２の機器では暗号器と第２の認証鍵の対、復号器と第１の機器の認証鍵の対が必要となる。また、機器の認証鍵についても第１の機器と第２の機器の違いは重要ではなく、ある特定の基準を満たす機器であることを他と区別する必要だけがある場合であったとしても、第１の機器にも第２の機器にも暗号器と認証鍵の対、および復号器と認証鍵の対が各１対必要となる。

【００３１】このように従来の機器間相互認証方式において特定の規格を満たす機器であることを相互に認証を行なう場合、各機器ごとに暗号器と認証鍵の対、および復号器と認証鍵の対、の２つの集積回路が必要となり機器のコストアップにつながるという問題点を有するものであった。

【００３２】上述のように特定規格を満たす機器であることを機器同士が確認して著作権データが規格外の機器に流出することを防止するためには、暗号器と認証鍵の対、および復号器と認証鍵の対の集積回路を設けることが効果的である。この場合、これらの集積回路はある管理の下で機器製造者に配布されなければならない。その管理とは正規の機器の製造にのみこれらの集積回路が利用されることを目的とした管理である。ところが、複数の機器製造者が存在する場合このような管理を完全に実施することは難しい。必ず、これらの集積回路を用いて不正な機器が製造される可能性がある。以下ではこの場合どのようなことが起こるかを考察する。

【００３３】暗号器・認証鍵対、および復号器・認証鍵対の各一対があれば正規の機器から著作権データを吸い上げる機器が実現できることは明らかである。ある不正な機器製造者がこのようにして不正なディジタル情報記録再生装置を作成したものとする。この装置は情報記録装置として動作するときには正規の機器から著作権データを吸い上げる。そして情報再生装置として動作するときには正規の機器に対して著作権データを吐き出す。このようにして著作権データの不正なコピーが可能となる。このことは、暗号器・認証鍵対と復号器・認証鍵対の両方を持つことに起因しているのである。

【００３４】このように、従来の機器間通信保護装置を実現しようとすると、不正な情報機器の製造を制限することが困難であるという問題点を有するものであった。

【００３５】また、従来の機器間通信のためには、通信リンクにより結合される機器の間でコマンドフェーズとデータ伝送フェーズを備えたものはあったが、前述のよ

うなコンパクトさと安全性を備えた特徴を持つものは存在しなかった。

【００３６】

【課題を解決するための手段】本発明は従来の機器間通信保護装置にあった上記のような欠点を改善するためになされたものであり、請求項１に係る発明は、通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証し通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換とし、一方の機器では前記認証プロトコルにおいて暗号変換であるのみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なう手段を有している。

【００３７】請求項２に係る発明は、通信リンクにより結合される機器の間で、暗号変換およびその逆変換を用いたチャレンジ・レスポンス型の認証プロトコルにより通信相手が適切な認証鍵をもつことを確認して通信相手の正当性を認証するとともに共通の暗号鍵を共有しこの暗号鍵を用いて暗号通信を行って通信リンク上のデータの保護を行う装置であって、前記暗号変換は平文全体の集合上への置換であり、一方の機器では前記認証プロトコルにおいて暗号変換のみを行ない、他方の機器においては前記プロトコルにおいて前記暗号変換の逆変換のみを行なう手段を有している。

【００３８】請求項３に係る発明は、請求項１および２の発明において、前記暗号変換および前記認証鍵からなる暗号変換モジュールと前記逆変換と前記認証鍵からなる逆変換モジュールをそれぞれモジュール外部からは前記暗号変換、前記逆変換および前記認証鍵が解析できないような構成とし、一方のモジュールを他方とは異なる管理基準の下に提供することを特徴としている。

【００３９】請求項４に係る発明は、請求項３の発明において、前記暗号変換、前記逆変換、および前記認証鍵とはそれぞれ異なる第２の暗号変換とこれに対応する第２の逆変換と第２の認証鍵からなるモジュールをモジュール外部からは前記第２の暗号変換と前記第２の逆変換と前記第２の認証鍵が外部からは解析できないような構成とし、これを通信リンクを介して通信する両方の機器に備え、これを前記認証プロトコルにおいて前記両方の機器において併用するものであり、前記変換モジュールおよび前記逆変換モジュールよりも厳しい管理基準の下に提供することを特徴としている。

【００４０】請求項５に関わる発明は、請求項２の発明において、通信リンクにより結合される機器の間で、コマンドフェーズとデータ伝送フェーズを備えており、前記コマンドフェーズで伝送するコマンドに認証と暗号鍵共有を起動するコマンドと、暗号通信コマンドを追加し、前記コマンドフェーズで認証と暗号鍵の共有を起動するコマンドを指定した場合に、続くデータ伝送フェーズで前記機器の間で通信相手の正当性を認証する処理と、その処理の結果として共通の暗号鍵の共有を行ない、次に暗号通信コマンドを指定した場合に、続く前記データ伝送フェーズで、前記共有した暗号鍵を用いてデータを暗号変換して伝送する構成としている。

【００４１】請求項６の発明は、請求項５の発明において、一旦リンクを分断して再度リンクを確立する機能を備え、分断前に再度リンクを確立する際の通信相手の正当性認証と暗号鍵共有と暗号伝送の、すべてまたは一部に関する情報を共有する手段を有している。

【００４２】

【発明の実施の形態】請求項１の発明は前記の構成をとることにより、認証プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【００４３】請求項２の発明は前記の構成をとることにより、認証および鍵共有プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【００４４】請求項３の発明は前記の構成をとることにより、暗号変換モジュールと暗号モジュール間、復号モジュールと復号モジュール間では認証ができないため、暗号モジュールまたは復号モジュールの一方の提供を厳重に管理することにより、装置間通信保護の効力を高めることができる。

【００４５】請求項４の発明は前記の構成をとることにより、前記暗号モジュールおよび復号モジュールとは異なる別のモジュールをより厳密な管理状態で提供することにより、装置間通信保護の効力を高めることができる。

【００４６】請求項５および６の発明は前記の構成をとることにより、機器間通信装置に正当性認証と暗号鍵共有と暗号伝送の保護機能のすべてまたはその一部の機能を追加することができる。

【００４７】（実施例１）図１は本発明の機器間通信保護装置の第１の実施例を示すブロック図である。

【００４８】図１において、７０は第１の機器、７１は第１の乱数発生部、７２は下記の条件を満たす暗号変換の暗号器、７３は機器認証鍵を格納する第１の認証鍵格納部であり、７２と７３は暗号モジュール７４として集積回路の形で一体化されている。７５は第１のデータ分離部、７６は第１のデータ比較部、７７は第３の乱数発生部、７８は第１のデータ連結部、７９は第１の共有鍵一時格納部、８０はデータ暗号器、８１は著作物データ格納部である。７１から８１は第１の機器の構成要素で

ある。８５は通信路である。９０は第２の機器、９１は前記暗号変換の復号器、９２は機器認証鍵を格納する第２の認証鍵格納部であり、９１と９２は復号実現モジュール９３として集積回路の形で一体化されている。９４は第２の乱数発生部、９５は第２のデータ連結部、９６は第２のデータ分離部、９７は第２のデータ比較部、９８は第２の共有鍵一時格納部、９９はデータ復号器、８９は著作物処理部である。９１から９９、８９は第２の機器の構成要素である。

【００４９】ここで前記暗号変換の満たすべき条件を述べる。暗号変換をＥ、Ｅに対する逆変換（復号変換）をＤとする。このとき，Ｅは平文全体の集合Ｓ１から暗号文全体の集合Ｓ２への写像，そしてＤはＳ２からＳ１への写像と考えられる。この時、ＥがＳ１上の置換であることが満たすべき条件である。

【００５０】写像Ｅが置換であるとは、以下の条件を満たすときにいう：

（１）Ｓ１＝Ｓ２、（２）Ｅが単射である、（３）Ｅが全射である。

【００５１】ここでＥが単射であるとは、「Ｓ１の元ｘ、ｙに対して、Ｅ（ｘ）＝Ｅ（ｙ）である場合は、ｘ＝ｙの場合に限る」ことをいう。またＥが全射であるとは、「任意のＳ２の元ｚに対して、あるＳ１の元ｗが存在して、Ｅ（ｗ）＝ｚを満たす」ことをいう。このとき、Ｅの復号アルゴリズムＤもＳ１上の置換となる。

【００５２】次にＥがＳ１上の置換である場合に満たす性質について述べる。まず全射Ｅが暗号アルゴリズムで、ＤがＥに対する復号アルゴリズムであることから、任意のＳ１の元ｘ、すなわち平文ｘ、に対して、暗号文Ｅ（ｘ）がＥの復号アルゴリズムＤで平文ｘに復号されるのであるから、

Ｄ（Ｅ（ｘ））＝ｘ　－－（＊１）

が成り立つ。ここで，Ｓ１＝Ｓ２であるから任意のＳ１の元ｘ、すなわち平文ｘ、に対して、Ｄ（ｘ）はＳ１の元となるから、上記（＊１）式のｘとしてＤ（ｘ）を取ると、

Ｄ（Ｅ（Ｄ（ｘ））＝Ｄ（ｘ）　－－（＊２）

が成り立つ。今、Ｅ、ＤがＳ１上の置換であるから、Ｄは単射である。よって式（＊２）から、

Ｅ（Ｄ（ｘ））＝ｘ　－－（＊３）

が成り立つ。すなわち、ある平文ｘに対してＤという（復号）変換を行った結果に対してＥという逆変換を行った結果は元に平文に戻る。このように、変換Ｄが一種の暗号変換になることが重要なポイントである。

【００５３】この実施例の機器間通信保護装置の動作を図２の動作説明図に従い説明する。本実施例は請求項２に対応するものである。

（１）まず、第１の機器７０は第１の乱数発生部７１において乱数Ｒ1を生成する。これは第１のチャレンジCHA1としての意味を持つ。そしてこれを通信路８５に対して送出する。

（２）第２の機器９０はこの電文CHA1（その内容は乱数Ｒ1である）を受けとると、第２の乱数発生器９４において第２の乱数Ｒ2を発生し、第２のデータ連結部９５において第１の乱数Ｒ1と第２の乱数Ｒ2を連結しこれを平文とし、第２の認証鍵格納部９２に格納されている機器認証鍵KSを復号鍵として復号器９１により復号変換する。

【００５４】RESCHA = D(KS, R1||R2)

ここで平文を復号変換するとは一種の暗号化を行うことを意味しており、その出力は乱数のように見える。ここでＲ2は第２のチャレンジとしての意味を持つ。復号化した結果は第１のチャレンジに対するレスポンスと第２のチャレンジの両方の意味を持つ。そしてその結果を通信路８５に対して送出する。

（３）この電文RESCHAを受けとった第１の機器７０はこのレスポンスデータを暗号文とし、第１の認証鍵格納部７３に格納されている機器認証鍵KSを暗号鍵として暗号器７２において暗号変換する。

【００５５】X1 = E(KS, RESCHA)

この場合の暗号変換とは前記復号変換の逆変換、すなわち復号化することに他ならない。そしてその結果X1を第１のデータ分離部７５に入力する。第１のデータ分離部７５は入力されたデータを第１の乱数部分RR1と第２の乱数部分RR2のデータに分離する。

【００５６】X1 : RR1 || RR2

そして第１の乱数部分のデータRR1を第１のデータ比較部７６に対して送出する。第１のデータ比較部７６はこのデータRR1を第１の乱数発生部７１に一時記憶されている乱数Ｒ1と比較する。これが一致すれば通信相手が正規の機器認証鍵KSを持っていることを証明したものと考え、通信相手が間違いなく正規機器であるものと認証し（４）に進む。もしも一致しなければここで認証処理を中断する。

（４）第３の乱数発生部７７は第３の乱数Ｋを発生する。第１のデータ連結部７８は第１のデータ分離部７５において分離された第２の乱数部分のデータRR2とこの乱数Ｋを連結し、これを暗号器７２に送り、暗号器７２はこの連結されたデータを平文とし、第１の認証鍵格納部７３に格納されている機器認証鍵KSを暗号鍵として暗号変換する。

【００５７】RES2 = E(KS, RR2||K)

そしてこの結果（第２のレスポンス）を通信路５５に対して送出する。

（５）この電文RES2を受けとった第２の機器６０はこのレスポンスデータを暗号文とし、第２の認証鍵格納部９２に格納されている機器認証鍵KSを復号鍵として前記暗号アルゴリズムの復号部９２において復号する。

【００５８】X2 = D(KS, RES2)

そしてその結果X2を第２のデータ分離部９６に入力する。第２のデータ分離部９６は入力されたデータX2を第

２の乱数部分のデータRRR2と第３の乱数部分のデータKKに分離する。

【００５９】X2 ： RRR2 || KK

そして第２の乱数部分のデータRRR2を第２のデータ比較部９７に対して送出する。第２のデータ比較部９７はこのデータRRR2を第２の乱数発生部９３に一時記憶されている乱数R2と比較する。これが一致すれば通信相手は正規の機器認証鍵を持っていることを証明したものと考え、通信相手が間違いなく正規の機器であることを認証する。そして（６）に進む。もしも一致しなければ認証は失敗したものとして認証処理を終る。

（６）第２のデータ分離部９６で分離された第３の乱数KK（これが乱数Kに等しいことは確認されている）を第２の共有鍵一時格納部９８に設定する。そして第１の機器７０に対して認証した旨の信号を送る。

（７）第２の機器９０から認証した旨の信号を受けた第１の機器７０は第３の乱数発生部７７で生成した乱数Kを第１の共有鍵一時格納部７９に転送する。そしてデータ暗号器８０は著作物データ格納部８１に格納されているデータをこの乱数Kを暗号鍵として用いて暗号化しその結果を通信路８５に対して送出する。

（８）この電文を受け取った第２の機器９０はデータ復号器９９に入力されるデータを第２の共有鍵一時格納部９８に格納されているデータを復号鍵として復号する。そしてこの結果を著作物処理部８９において処理する。

【００６０】第１の機器７０と第２の機器９０がどちらも正当なものであれば共有鍵一時格納部６８に格納されているデータは前記第１の共通鍵一時格納部に格納されているデータと等しくなるので（８）のステップで暗号化されたデータが正しく復号される。

【００６１】もしも第１の機器が正規の認証鍵を有し、第２の機器が正規の認証鍵を有していない場合、ステップ（３）で第１の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理が中断される。また第１の機器が正規の認証鍵を有しておらず、第２の機器は正規の認証鍵を有している場合、ステップ（５）において第２の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断する。従って、第２の共有鍵一時格納部には正しい共有鍵が設定されない。このようにして著作権データが不正な機器に流出することとともに不正な機器から正規の機器に流入することが防止できる。

【００６２】また、第１の機器も第２の機器も正当な認証鍵を有している場合で、認証処理が完了し、ステップ（７）（８）において著作権データが通信路上を伝送されているものを電気的にコピーしてディジタル蓄積装置に蓄積したとしてもそのディジタルデータは暗号化されており、無意味なものなので著作権データを有効に保護できる。

【００６３】本実施例では第１の機器では暗号器と認証鍵の対、第２の機器では復号器と認証鍵の対、だけが必要となる。これは従来の機器間通信保護装置が第１の機器にも第２の機器にも暗号器と認証鍵の対、および復号器と認証鍵の対が各１対必要となることと比較すると集積回路が１つでよく機器のコストダウンにつながるという効果がある。

【００６４】さらに、暗号器と認証鍵の対となる集積回路、および復号器と認証鍵の対となる集積回路はある管理の下で機器製造者に配布されなければならない。その管理とは正規の機器の製造にのみこれらの集積回路が利用されることを目的とした管理である。ところが、複数の機器製造者が存在する場合このような管理を完全に実施することは難しい。必ず、これらの集積回路を用いて不正な機器が製造される可能性がある。以下ではこの場合どのようなことが起こるかを考察する。

【００６５】暗号器・認証鍵対の集積回路は厳重な管理の下で機器製造者に提供されるものとしよう。一方復号器・認証鍵対の集積回路は前記管理ほど厳重ではない形で機器製造者に提供されるものとしよう。このとき暗号器・認証鍵対の集積回路は光ディスクなどに格納されている著作権データを受け取りこれを通信リンクを介して提供する側の機器（これを提供側機器とよぶ）に設置するものとし、復号器・認証鍵対の集積回路は前記機器から通信リンクを介して著作権データの提供を受ける側の機器（これを獲得側機器とよぶ）に設置するものと決めておく。前述のように暗号器・認証鍵対の集積回路は厳重な管理の下で提供側機器製造者に提供されるので正規の提供側機器しか作成できない。一方復号器・認証鍵対の集積回路は前記管理ほど厳重ではない形で機器製造者に提供されるため、ある不正な機器製造者が本来の契約に反して獲得側および提供側の両方の性質をもった機器を作成する可能性がある。例えば不正なディジタル情報記録再生装置を作成しようとしたものとする。この装置は情報記録装置として動作するときには正規の提供側機器から著作権データを獲得する機器である。復号器・認証鍵対の集積回路があるから前記の双方向認証が可能となり正規の提供側機器から著作権データを獲得することができる。一方、情報再生装置として動作するときには正規の獲得側機器に対して著作権データを提供することが必要である。ところが著作権データの獲得側機器には復号器・認証鍵対しか備えられていないため著作権データの提供のためには暗号器・認証鍵対の集積回路が必要となる。前述のように厳密な管理によりこのような集積回路が入手できないので結局このような不正な機器を作成することができない。以上の説明は請求項３に関わる。

【００６６】なお、本実施例においては双方向の認証の後に鍵共有を行うものとしたが暗号通信の必要のない場合にはこの部分は割愛することができる。これは請求項１に関わる。

【００６７】また、本実施例においては、チャレンジは平文、レスポンスは暗号文（復号文）という場合であり、さらに第２の機器から第１の機器への第１のレスポンスと第２のチャレンジを合成したプロトコルを説明したが、本発明の認証プロトコルはこの方法に限定されるものではなく、チャレンジは乱数を暗号化（復号化）したもの、レスポンスはこれを復号化（暗号化）したものというようにすることも可能である。本発明のポイントは認証プロトコルの如何によらず一方の機器には暗号化モジュールまたは復号化モジュールのいづれか一方しかないことによりコストダウンを図りさらにこのモジュールの不正使用に対する安全性を増したところにある。

【００６８】（実施例２）図３は本発明の機器間通信保護装置の第２の実施例を示すブロック図である。同図を図１と比べると第１の機器７０においては第２の暗号アルゴリズムの暗号器８２および第２の機器認証鍵KS2を格納する第５の認証鍵格納部８３が追加されている。この２つの構成要素は第２の暗号モジュール８４として集積回路などの形で一体化されている。第２の機器９０においては第２の暗号アルゴリズムの暗号器１０１および第２の機器認証鍵KS2を格納する第６の認証鍵格納部１０２が追加されている。この２つは第３の暗号モジュール１０３として集積回路などの形で一体化されている。これ以外は図１の対応する番号の構成要素と同じである。

【００６９】ここで第２の暗号アルゴリズムは第１の実施例で述べた置換の性質を備える必要はなく、一般の暗号アルゴリズム（本明細書の従来技術で述べたもの）でよい。ただし後述のようにこの場合はこの暗号モジュールが不正利用されないように厳重に管理されなければならない。

【００７０】第２の実施例の機器間通信保護装置の動作を図４の動作説明図に従い説明する。本実施例は請求項４に対応するものである。

（１）まず、第１の機器７０は第１の乱数発生部７１において乱数R1を生成する。これは第１のチャレンジCHA1としての意味を持つ。そしてこの電文CHA1を通信路８５に対して送出する。

（２）第２の機器９０はこの電文CHA1（その内容は乱数R1）を受けとると、これを第２の暗号アルゴリズムの暗号器１０１の入力とする。第２の暗号アルゴリズムの暗号器１０１は第６の認証鍵格納部に格納されている第２の機器認証鍵KS2を鍵として暗号化を行って暗号文データを作成する。

【００７１】X1 = e(KS2, R1)

一方第２の乱数発生器９４において第２の乱数R2を発生し、第２のデータ連結部９５において前記暗号文データX1と第２の乱数R2を連結し、これを平文として、第２の認証鍵格納部９２に格納されている機器認証鍵KSを復号鍵として暗号アルゴリズムの復号器９１により復号変換する。

【００７２】RESCHA = D(KS, X1||R2)

ここで平文を復号変換するとは一種の暗号化を行っていることに他ならなず、その出力は乱数のように見える。ここでR2は第２のチャレンジとしての意味を持つ。復号変換した結果は第１のチャレンジに対するレスポンスおよび第２のチャレンジの両方の意味を持つ。そしてその結果RESCHAを通信路８５に対して送出する。

（３）この電文RESCHAを受けとった第１の機器７０はこのデータを暗号文とし、第１の認証鍵格納部７３に格納されている認証鍵KSを暗号鍵として暗号器７２において暗号変換する。この場合の暗号変換とは平文に戻すことである。

【００７３】X2 = E(KS, RESCHA)

そしてその結果X2を第１のデータ分離部７５に入力する。第１のデータ分離部７５は入力されたデータX2を前記暗号文データ部分XX1と第２の乱数部分のデータRR2に分離する。そして前記暗号文データ部分のデータXX1を第１のデータ比較部７６に対して送出する。一方第１の乱数発生部７１に一時記憶されている乱数R1は第２の暗号アルゴリズムの暗号器８２に送られここで第５の認証鍵鍵格納部８３に格納されている第２の機器認証鍵KS2を暗号鍵として暗号化される。

【００７４】X3 = e(KS2, R1)

その結果X3は第１のデータ比較部７６において前記暗号文データ部分のデータXX1と比較される。これが一致すれば通信相手が第２の機器９０の認証鍵および第２の認証鍵を持っていることを証明したものと考え、通信相手が間違いなく正規の機器であるものと認証し（４）に進む。もしも一致しなければここで認証処理を中断する。

（４）第２の暗号アルゴリズムの暗号器８２は第１のデータ分離部７５において分離された第２の乱数部分のデータRR2を入力とし第５の認証鍵格納部８３に格納されている第２の機器認証鍵KS2を鍵として暗号化を行って暗号文データを作成する。

【００７５】X4 = e(KS2, RR2)

一方第３の乱数発生部７７は第３の乱数Kを発生する。そして暗号アルゴリズムの暗号器７２は前記データX4この乱数Kを第１のデータ連結部７８において連結したものを平文とし、第１の認証鍵格納部７３に格納されている機器認証鍵を暗号鍵として暗号化する。

【００７６】RES2 = E(KS, X4||K)

そしてこの結果を第２のレスポンスRES2としてを通信路５５に対して送出する。

（５）この電文を受けとった第２の機器６０はこのレスポンスデータを暗号文とし、第２の認証鍵格納部９２に格納されている機器認証鍵KSを復号鍵として前記暗号アルゴリズムの復号部９２において復号する。

【００７７】X5 = D(KS, RES2)

そしてその結果X5を第２のデータ分離部９６に入力す

る。第２のデータ分離部９６は入力されたデータX5を第２の乱数部分XX4と第３の乱数部分のデータKKに分離する。そして第２の乱数部分のデータXX4を第２のデータ比較部９７に対して送出する。一方第２の乱数発生部９４に一時記憶されている乱数R2は第２の暗号アルゴリズムの暗号器１０１に送られここで第６の認証鍵鍵格納部１０２に格納されている第２の機器認証鍵KS2を暗号鍵として暗号化される。

【００７８】X6 = e(KS2,R2)

このデータX6は第２のデータ比較部９７に送られ第２のデータ比較部９７はこのデータを前記データXX4と比較する。これが一致すれば通信相手は正規の機器認証鍵を持っていることを証明したものと考え、通信相手が間違いなく正規の機器であることを認証する。そして（６）に進む。もしも一致しなければ認証は失敗したものとして認証処理を終る。

（６）第２のデータ分離部で分離された第３の乱数を第２の共有鍵一時格納部９８に設定する。そして第１の機器７０に対して認証した旨の信号を送る。

（７）第２の機器９０から認証した旨の信号を受けた第１の機器７０は第３の乱数発生部７７で生成した乱数Kを第１の共有鍵一時格納部７９に転送する。そしてデータ暗号器８０は著作物データ格納部８１に格納されているデータをこの乱数Kを暗号鍵として用いて暗号化しその結果を通信路８５に対して送出する。

（８）この電文を受け取った第２の機器９０はデータ復号器９９に入力されるデータを第２の共有鍵一時格納部９８に格納されているデータを復号鍵として復号する。そしてこの結果を著作物処理部８９において処理する。

【００７９】もしも第１の機器が正規の認証鍵をすべてを有し、第２の機器が正規の認証鍵のうち有していないものがある場合、ステップ（３）で第１の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理が中断される。また第１の機器が正規の認証鍵のうちいずれかは有しておらず、第２の機器は正規の認証鍵をすべて有している場合、第２の機器は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断する。このようにして著作権データが不正な機器に流出することとともに不正な機器から正規の機器に流入することが防止できる。

【００８０】この第２の実施例のポイントは、第１の実施例における暗号モジュールおよび復号モジュールとは異なる暗号変換および第２の認証鍵からなるモジュールを通信リンクに接続される両方の機器に備え、これを双方向認証プロトコルに併用したことにある。従って、第２の暗号器と第２の認証鍵を厳重に管理することにより、第１の実施例よりもさらに厳重な機器認証を行うことができる。

【００８１】前記暗号モジュールと復号モジュールは通信リンクの両端に備わる通信制御のための集積回路に組み込まれることにより効果的に実現することができる。一方、第２の暗号器と第２の認証鍵は前記暗号モジュールや復号モジュールよりもさらに厳重に管理されるべきであり、例えばシステムコントローラ用の集積回路に組み込まれることにより最も効果的に実現される。

【００８２】なお、本実施例においては第２の暗号モジュールを第１および第２の機器に組み込み認証処理に関与させることについて説明したが、本発明はこの構成に限定されるものではなく、例えば第１の機器にはある暗号アルゴリズムの暗号モジュールを追加し、第２の機器にはこれに対応する復号モジュールを追加してこのモジュールにおける処理を双方向認証プロトコルに組み込むことも可能である。本発明の重要な点はこれらを厳重に管理することにより機器間通信保護装置の安全性をより高めることができることにある。

【００８３】（実施例３）次に、以上述べた機器間通信保護装置を例えば、代表的な標準入出力インタフェースであるSCSI（Small Computer System Interfaceの略語）を用いたデータ伝送に適用した第３の実施例について説明する。本実施例は請求項５に対応するものである。

【００８４】SCSIではある１対の機器は、バスを占有した後、コマンド、データ、ステータス、メッセージの４つのフェーズを遷移しながらデータを伝送する。例えば、第１の機器が第２の機器からデータを読み込む場合の典型的なフェーズ遷移は次のとおりである。

（１）コマンドフェーズ：第１の機器が第２の機器に対して、データ読み込みのコマンドを送出。

（２）データフェーズ：第２の機器から第１の機器に指定の長さのデータが送られる。

（３）ステータスフェーズ：第２の機器から第１の機器にコマンド実行結果の報告。

（４）メッセージフェーズ：第２の機器から第１の機器にコマンド終了メッセージ送出。

【００８５】第３の実施例では、このコマンドに新たに認証と暗号鍵共有のコマンドと暗号通信コマンドを追加する。これらのコマンドを用いた第３の実施例の機器間通信保護装置の動作を、図５の第１の機器と第２の機器のやりとりを示す図に従い説明する。図５において１２０は第１の機器、１２１は第２の機器であり、その間のやりとりを上から順に示している。なお、図５では第１の機器が第２の機器からデータを読み込む場合について示す。

（１）コマンドフェーズ：第１の機器が第２の機器に対して、認証と暗号鍵共有のコマンドを送出する。

（２）データフェーズ：第１の機器と第２の機器の間で第２の実施例に従ったデータのやりとりを行なう。

【００８６】(1)のコマンドに従い、第１の機器と第２の機器はチャレンジ・レスポンスのやりとりを行ない、片側または相互に通信相手の正当性を認証する。そし

て、この処理の結果として共通の暗号鍵を共有する。

（３）ステータスフェーズ：第２の機器から第１の機器に（１）のコマンド実行結果の報告。

（４）メッセージフェーズ：第２の機器から第１の機器に（１）のコマンド終了メッセージ送出。

（５）コマンドフェーズ：第１の機器が第２の機器に対して、暗号通信（読み込み）コマンドを送出する。

（６）データフェーズ：第２の機器から第１の機器に指定の長さのデータが送られる。

【００８７】このとき、（５）のコマンドに従って、第２の機器は（２）で共有した共通の暗号鍵を用いてデータを暗号化して伝送する。第１の機器は伝送されたデータを受けとって、共通の暗号鍵で復号する。

（７）ステータスフェーズ：第２の機器から第１の機器に（５）のコマンド実行結果の報告。

（８）メッセージフェーズ：第２の機器から第１の機器に（５）のコマンド終了メッセージ送出。

【００８８】なお、以上の説明ではSCSIをもとに説明を行なったが、何もそれに特定するわけではなく、上記のうちコマンドフェーズとデータフェーズを備える入出力インタフェーズであれば、そのコマンドに通信保護のためのコマンドを追加してデータフェーズで認証や暗号鍵の共有や暗号通信をすることにより実現できる。

【００８９】また、SCSIではSCSIバスの有効利用のため、ディスコネクトとリコネクトの機能が備わっている。例えば大量のデータをディスクからの読み出すコマンドを実行する場合に、途中にシーク時間（ヘッド位置の移動のための時間）が入る場合がある。この間はデータの読みだしはできないので、バスが空いたままになってしまう。バスの使用効率を向上するため、こういった場合、一旦機器間のリンクを分断（ディスコネクト）して、他の機器に解放し、再びバスを使用する準備ができたら再度接続（リコネクト）を要求する。

【００９０】第３の実施例でこのディスコネクトとリコネクト機能を備える場合には、ディスコネクトの前に相互の機器の間で、リコネクトの時に認証、暗号鍵共有、暗号通信を同いった手順で行なうのかを打ち合せる。このことは請求項６に関するものである。上記打ち合せる内容は例えば次のようなものである。

・リコネクトしたときに、上で述べた手順に従って再度通信相手の正当性の認証処理を行なうか。それとも簡易版として片側だけの認証を行なうのか。それとも行なわないのか。

・リコネクトしたときに、上で述べた手順に従って再度共通の暗号鍵の設定を行なうか。それとも以前の暗号鍵を用いるか。この打合せを行なってからディスコネクトすることにより、リコネクトの際の双方のやりとりをスムーズに行なうことができる。

【００９１】

【発明の効果】以上のように請求項１の発明は、認証プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【００９２】請求項２の発明は、認証および鍵共有プロトコルを実現するとき、一方の機器では暗号変換のみを行ない、他方の機器においては前記暗号変換の逆変換のみを行なうことが可能となり、暗号変換とその逆変換の両方を有する必要がなくコンパクトに実現できるようになった。

【００９３】請求項３の発明は、暗号変換モジュールと暗号モジュール間、復号モジュールと復号モジュール間では認証ができないため、暗号モジュールまたは復号モジュールの一方の提供を厳重に管理することにより、装置間通信保護の効力を高めることができる。

【００９４】請求項４の発明は前記暗号モジュールおよび復号モジュールとは異なる別のモジュールをより厳密な管理状態で提供することにより、装置間通信保護の効力を高めることができる。

【００９５】請求項５および６の発明は、従来の機器間通信装置に正当性認証と暗号鍵共有と暗号伝送の保護機能のすべてまたはその一部の機能を追加したときに、上記の効果を発揮することがすることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施例のブロック図

【図２】本発明の第１の実施例の動作説明図

【図３】本発明の第２の実施例のブロック図

【図４】本発明の第２の実施例の動作説明図

【図５】本発明の第３の実施例の動作説明図

【図６】従来の機器間通信保護装置の一例のブロック図

【図７】従来の機器間通信保護装置の一例の動作説明図

【図８】従来の機器間通信保護装置の他の例のブロック図

【図９】従来の機器間通信保護装置の他の例の動作説明図

【符号の説明】

７１　第１の乱数発生器

７２　暗号器

７３　第１の認証鍵格納部

７４　暗号モジュール

７６　第１のデータ比較部

９１　復号器

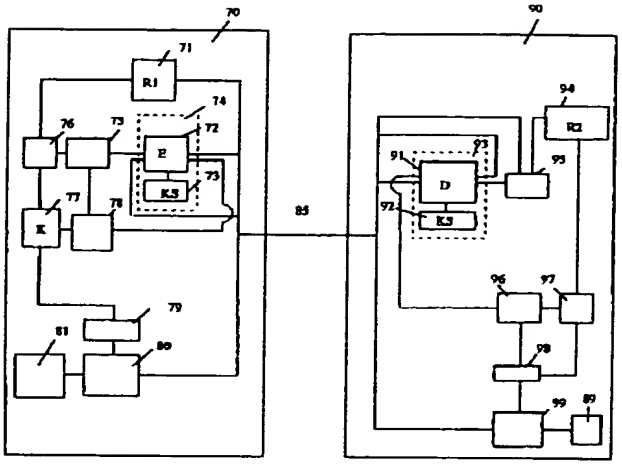
９２　第２の認証鍵格納部

９３　復号モジュール

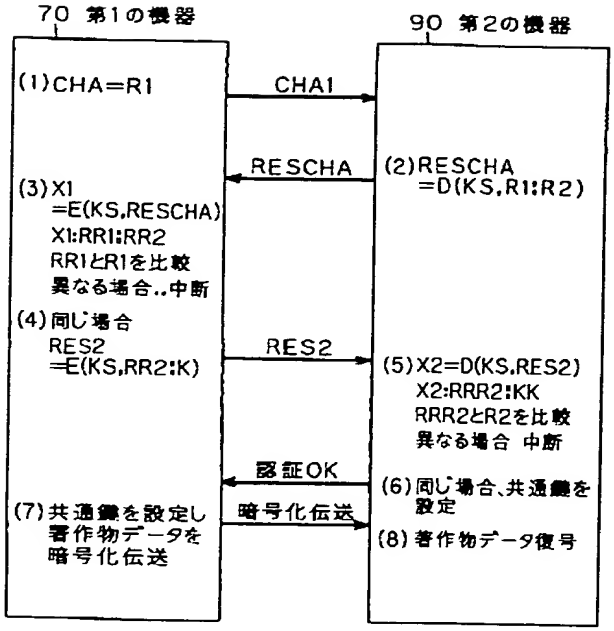
９４　第２の乱数発生部

９７　第２のデータ比較部

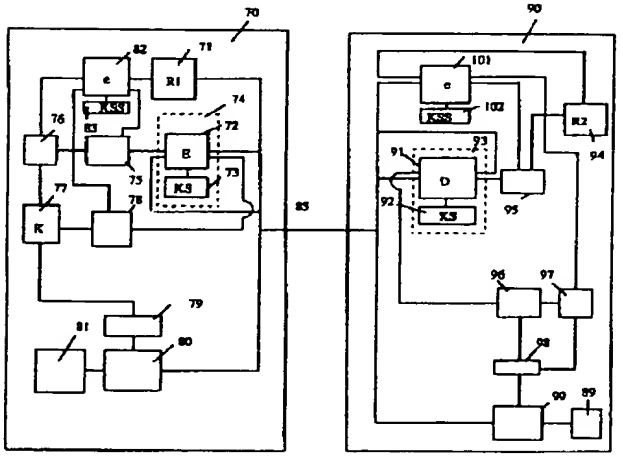
【図１】


70
71
R1
74
72
E
76
73
KS
77
78
K
79
81
80
85
90
94
R2
91
93
D
95
92
K3
96
97
98
99
89

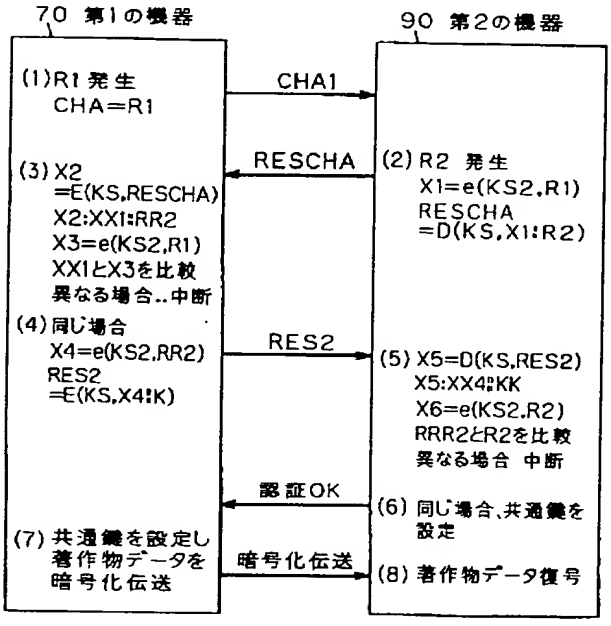
【図２】


70 第1の機器
90 第2の機器
(1)CHA=R1
CHA1
RESCHA
(2)RESCHA
=D(KS,R1:R2)
(3)X1
=E(KS,RESCHA)
X1:RR1:RR2
RR1とR1を比較
異なる場合..中断
(4)同じ場合
RES2
=E(KS,RR2:K)
RES2
(5)X2=D(KS,RES2)
X2:RRR2:KK
RRR2とR2を比較
異なる場合 中断
認証OK
(6)同じ場合、共通鍵を
設定
(7)共通鍵を設定し
著作物データを
暗号化伝送
暗号化伝送
(8)著作物データ復号

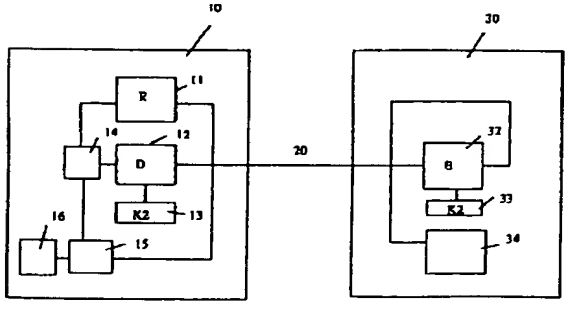
【図３】


70
82
e
KS1
71
R1
74
72
E
76
83
73
KS
77
78
K
79
81
80
85
90
101
e
KS2
102
R2
94
91
93
D
95
92
K3
96
97
98
90
89

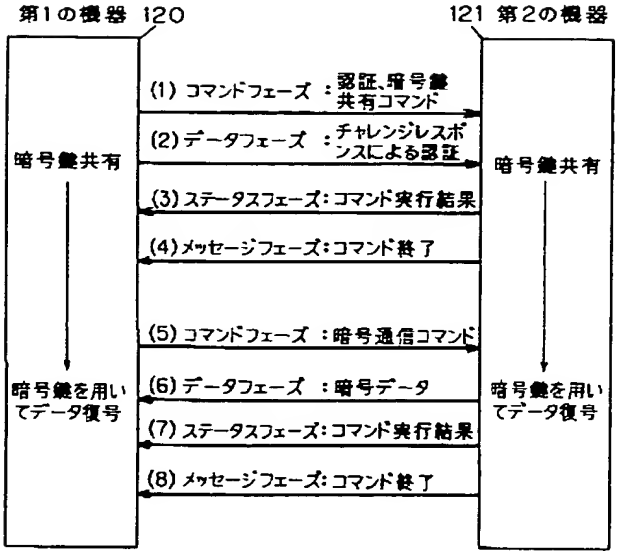
【図４】


70 第1の機器
90 第2の機器
(1)R1 発生
CHA=R1
CHA1
RESCHA
(2) R2 発生
X1=e(KS2,R1)
RESCHA
=D(KS,X1:R2)
(3) X2
=E(KS,RESCHA)
X2:XX1:RR2
X3=e(KS2,R1)
XX1とX3を比較
異なる場合..中断
(4)同じ場合
X4=e(KS2,RR2)
RES2
=E(KS,X4:K)
RES2
(5) X5=D(KS,RES2)
X5:XX4:KK
X6=e(KS2,R2)
RRR2とR2を比較
異なる場合 中断
認証OK
(6) 同じ場合、共通鍵を
設定
(7) 共通鍵を設定し
著作物データを
暗号化伝送
暗号化伝送
(8) 著作物データ復号

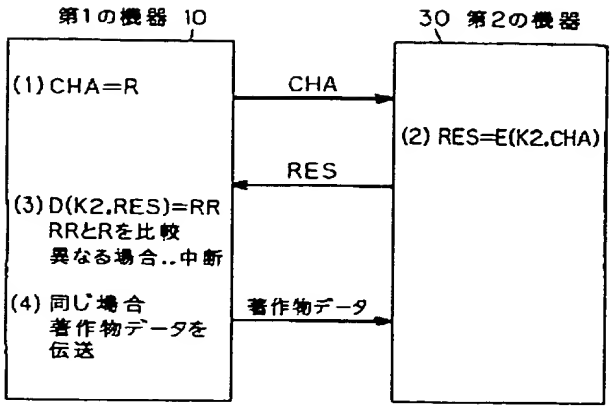
【図６】


10
11
R
14
12
D
16
K2
13
15
20
30
32
E
33
K2
34

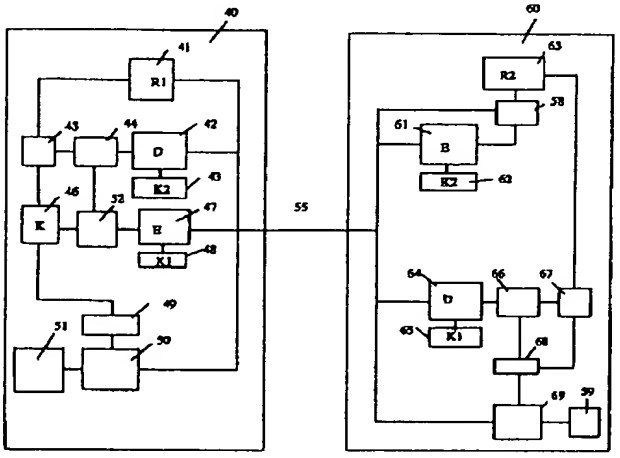
【図５】



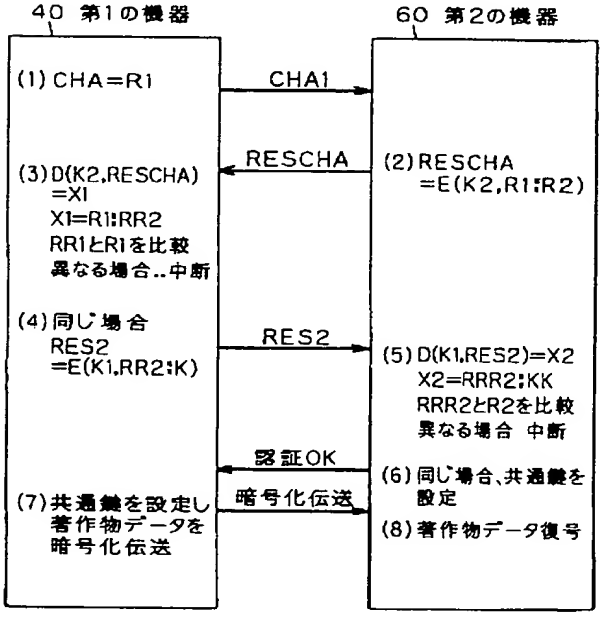
【図７】



【図８】



【図９】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
			H04L 9/00	675B

(72) 発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72) 発明者　小塚　雅之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72) 発明者　山内　一彦
大阪府門真市大字門真1006番地　松下電器産業株式会社内